Status of the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application

1. (Currently Amended) A method for verifying that a source device that is capable of receiving protected content is authorized to communicate the protected content to a sink device that is capable of descrambling the protected content comprising:

receiving at said source device an approval code associated with said source and sink devices;

determining, in said source device, a local code using data associated with said source and sink devices; and

comparing, in said source device, at least a portion of said approval code to at least a portion of said local code, ~~and~~ verifying that the sink device is authorized to receive the protected content from said source device in response to the comparison, and providing access to the protected content to the sink device in response to the verifying step.

2. (Original) The method according to claim 1. wherein said approval code is determined based on a hash calculation using identifiers uniquely associated with said source and sink devices and wherein said local code is determined based on a hash calculation using data from said sink device and a source identifier prestored in said source device.

3. (Original) The method according to claim 2, wherein said data associated with said source device for determining said local code is not public information and wherein said data associated with said sink device for determining said local code is public information.

4. (Original) The method of Claim 2, wherein said identifiers are serial numbers or other identification codes accessible to a user, and wherein said data from said sink device used in said hash calculation is a public key.

5. (Currently amended) A method for verifying that a source device that is capable of receiving protected content is authorized to communicate protected content to a sink device that is capable of descrambling the protected content comprising:

providing substantially unique identifiers associated with said source and sink devices to a validation authority

receiving from said validation authority an approval code, said approval code using data corresponding to said identifiers;

determining, in said source device, a local code using said data associated with said source and sink devices, and

comparing at least a portion of said approval code to at least a portion of said local code, ~~and~~ verifying that the sink device is authorized to receive the protected content from the source device in response to the comparison, and providing access to the protected content to the sink device in response to the verifying step.

6. (Original) The method of Claim 5, further comprising said validation authority providing said at least portion of said approval code to a user, and said user providing said at least portion of said approval code to said source device.

7. (Original) The method of Claim 5, wherein said substantially unique identifiers are provided to said validation authority by said user.

8. (Original) The method of Claim 5, wherein said source device is selected from one of an access device and a media player and wherein said sink device is a digital television.

9. (Original) The method of Claim 5, wherein said data associated with said source device is secured so as not to be readily ascertainable by said user.

10. (Original) The method of Claim 5, wherein said data associated with said source and sink devices comprises a unique identification indicative of said source device and a public encryption key associated with said sink device.

11. (Original) The method of Claim 10, wherein said unique identification indicative of said source device is secured from a user of said source device.

12. (Original) The method of Claim 1, further comprising said source device communicating whether said source device is authorized to provide said content to said sink device to a user, and intentionally delaying communicating whether or not said compared approval code and local code are consistent.

13. (Currently amended) A method for verifying that a selected device is authorized to receive protected content and for selecting at least one security key and at least one identifier used to access protected content, said method comprising:

receiving at a first device a plurality of security keys associated with said content;

receiving said identifier at said first device to be used to provide said content to a second device, said identifier being associated with said second device;

comparing said identifier with said plurality of security keys and verifying that said second device is authorized to receive said protected content in response to the comparison, and selecting one of said plurality of security keys associated with said identifier using said first device; and,

providing said content to said second device using said first device and selected security key in response to verifying that said second device is authorized to receive said protected content.

14. (Original) The method according to claim 13, comprising providing a serial identification indicative of said second device for accessing said content to a validation authority.

15. (Original) The method according to claim 14, further comprising determining an identifier associated with said second device using said serial identification.

16. (Original) The method of Claim 13, wherein said plurality of security keys are indexed in a table of keys and said identifier is the index of said select key in the table of keys and a result of a hash function of said identifier.

17. (Currently amended) A method for verifying that a source device, having an associated substantially unique identifier and serial number and a sink device having a

substantially unique key and serial number should have access to content by using a validation authority, wherein said unique identifier is secured by a user of said source device, said method comprising:

providing said serial numbers to said validation authority;

said validation authority determining said substantially unique identifier using said serial numbers; and, if said access to said content is authorized,

said validation authority determining an authorization identifier using said substantially unique identifier,

said source device determining a local identifier using said substantially unique identifier; and,

verifying said source device and sink device are authorized to have access to content if said authorization identifier and local identifier correspond to one another, and providing access to the protected content to the sink device in response to the verifying step.

18. (Original) The method of Claim 17, further comprising said validation authority providing said at least portion of said authorization identification to a user, and said user providing said authorization identification to said source device.

19. (Currently amended) A method for verifying that a set top box is authorized to communicate protected content to a digital television comprising:

receiving at said set top box an approval code associated with said set top box and said digital television;

determining, in said set top box, a local code using data associated with said set top box and said digital television; and

comparing at least a portion of said approval code to at least a portion of said local code, ~~and~~ verifying that said digital television is authorized to receive said protected content from said set top box in response to the comparison, and providing access to the protected content to the digital television in response to the verifying step.

20. (Original) The method of claim 19, wherein the approval code is generated using the respective serial numbers of the set top box and the digital television.

21. (Currently amended) A method for verifying that a digital video recorder is authorized to communicate protected content to a digital television comprising:

receiving at said digital video recorder an approval code associated with digital video recorder and said digital television;

determining, in said digital video recorder, a local code using data associated with said digital video recorder and said digital television; and

comparing at least a portion of said approval code to at least a portion of said local code, ~~and~~ verifying that said digital television is authorized to receive said protected content from said digital video recorder in response to the ~~comparision~~ comparison, and providing access to the protected content to the digital television in response to the verifying step.

22. (Original) The method of claim 21, wherein the approval code is generated using the respective serial numbers of the digital video recorder and the digital television.